NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PASCAL POLYNOMIALS OVER GF(2)

by

Carlos K. Fernandez

June 2008

Thesis Co-Advisors:	Harold M. Fredricksen Pantelimon Stanica

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** June 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Pascal Polynomials Over GF(2) **6. AUTHOR(S)** Carlos K. Fernandez	**5. FUNDING NUMBERS**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) NA	**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The Discrete Logarithm Problem (DLP) is a fundamental cryptographic primitive. The DLP is defined for any cyclic group, specifically finite fields, whether the integers modulo a prime p or a polynomial field of characteristic p modulo some irreducible polynomial $f(x)$. For polynomial fields over a finite field, also known as Galois fields, the DLP can be viewed as finding a solution to the equation $1 + x^i = x^j$ for arbitrary values of i (modulo some primitive polynomial). Solutions are (relatively) easy to find for trinomials and these would be the easiest polynomials to implement in hardware. However, primitive trinomials do not exist for all degrees.

Primitive polynomials are irreducible polynomials with an associated primitive root α that is a generator of the multiplicative group. Thus the generator α generates all nonzero $2^n - 1$ elements of a Galois field whose base field is the integers modulo two. Primitive polynomials over the field of two elements, or $GF(2)$, have important applications in cryptology and coding theory.

This thesis investigates properties of polynomials with more than three terms where all but one term is a row of Pascal's triangle modulo two. In other words we define a certain class of polynomials by $f(x) = x^n + p(x)$, where $p(x)$ is a row of Pascal's triangle modulo two. This thesis shows that some of these polynomials, which are not trinomials, also have "easy" solutions. We observe that for a polynomial to have an associated primitive element, there are definite restrictions on the degree of the polynomial using particular rows of Pascal's triangle.

14. SUBJECT TERMS Discrete Mathematics, Abstract Algebra, Number Theory, Galois Fields, Linear Feedback Shift-Registers	**15. NUMBER OF PAGES** 71
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

PASCAL POLYNOMIALS OVER GF(2)

Carlos K. Fernandez
Major, United States Army
B.S., United States Military Academy, 1997

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN APPLIED MATHEMATICS

from the

NAVAL POSTGRADUATE SCHOOL
June 2008

Author: Carlos K. Fernandez

Approved by: Dr. Harold M. Fredricksen
Thesis Co Advisor

Dr. Pantelimon Stanica
Thesis Co Advisor

Dr. Clyde L. Scandrett
Chairman, Department of Applied Mathematics

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The Discrete Logarithm Problem (DLP) is a fundamental cryptographic primitive. The DLP is defined for any cyclic group, specifically finite fields, whether the integers modulo a prime p or a polynomial field of characteristic p modulo some irreducible polynomial $f(x)$. For polynomial fields over a finite field, also known as Galois fields, the DLP can be viewed as finding a solution to the equation $1 + x^i = x^j$ for arbitrary values of i (modulo some primitive polynomial). Solutions are (relatively) easy to find for trinomials and these would be the easiest polynomials to implement in hardware. However, primitive trinomials do not exist for all degrees.

Primitive polynomials are irreducible polynomials with an associated primitive root α that is a generator of the multiplicative group. Thus the generator α generates all nonzero $2^n - 1$ elements of a Galois field whose base field is the integers modulo two. Primitive polynomials over the field of two elements, or $GF(2)$, have important applications in cryptology and coding theory.

This thesis investigates properties of polynomials with more than three terms where all but one term is a row of Pascal's triangle modulo two. In other words we define a certain class of polynomials by $f(x) = x^n + p(x)$, where $p(x)$ is a row of Pascal's triangle modulo two. This thesis shows that some of these polynomials, which are not trinomials, also have "easy" solutions. We observe that for a polynomial to have an associated primitive element, there are definite restrictions on the degree of the polynomial using particular rows of Pascal's triangle.

THIS PAGE INTENTIONALLY LEFT BLANK

DISCLAIMER

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank the entire Staff and Faculty at the Naval Postgraduate School's Applied Mathematics Department. Everyone there, directly or indirectly, helped me to successfully complete the program. I would particularly like to thank my advisors Dr. Hal Fredricksen and Dr. Pante Stanica for their support and guidance throughout this writing process. Pante's particular attention to the details and insightful approach greatly simplified many ideas I attempted to convey in these following pages. No less attentive or demanding, Hal is a great inspirator, motivator, and friend. Thank you for the many talks, hours and words of wisdom. It has truly been a pleasure to work with you all, and I hope we meet again someday.

A special thanks goes to Dr. Floyd "Ben" Cole and his colleague Dr. James R. Schatz. Ben provided me some much needed encouragement to finally finish this undertaking, while Jim provided the keys to the proof in Appendix A.

I would also like to thank my friends and family, who were always supportive of me and helped me to fulfill my goals and dreams. Firstly, many thanks to my officemate, classmate, and good friend Major Douglas "Chip" Fletcher. You were always there to listen to my crazy ideas and ramblings as I hope I did for you too. I would also like to thank my daughter Panthea and son Aiden. Although they never understood why dad wasn't home (or why he was so grumpy when he was) because he was studying or taking a test or working on projects, hopefully I can make it up to them someday. Most importantly, I thank my wife Colleen. You are truly my better half. Even though it was VERY difficult with us both having been in school at the same time, we made it work. I hope I can support you and your dreams as you have for me for so many years.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

Digital communications are now commonplace, if not essential, in our day to day lives. The average user takes for granted the inner workings of their computer systems. One feature in particular is random-number generation, which computer software systems utilize in cryptographic library files. The simplest and most efficient method for random-number generation is via a maximum period Linear-Feedback Shift Register (LFSR). The authoritative source on the topic is *Shift Register Sequences* by Solomon W. Golomb [1]. These pseudo-random sequences, also called m-sequences, have the needed randomness properties of balance, runs, and correlation. Applications of LFSR's range from stream ciphers to scrambling sequences used by cable television, satellite communications and cell-phones. Each m-sequence is uniquely determined by a primitive polynomial whose coefficients are elements of some prime sub-field, p. We call this subfield the Galois field with p elements, denoted by $GF(p)$. We restrict our attention to the case $p = 2$ in this thesis. These polynomials are useful for a wide variety of applications such as random-number generators, stream ciphers, and linear code generators.

Specifically, primitive polynomials are essential to Error Checking and Correcting (ECC) Hamming Codes and the Advanced Encryption System (AES) [2]. One area of particular interest to the Cryptologic and Coding communities is the Discrete Logarithm Problem (DLP) [3]. While logarithms are straightforward to find over the real numbers, the DLP looks for solutions to the following equation modulo some polynomial $f(x)$ whose coefficients are taken modulo some prime p. So we define the DLP over $GF(2^n)$ in the following way; for a primitive polynomial $f(x)$ of degree n with root α, an integer i, and the relation $1 + x^i = x^j$, solve for j in a computationally feasible amount of time. This relation implies that the polynomial $g(x) = x^j + x^i + 1$ is a trinomial multiple of $f(x)$, or that $f(x)$ divides $g(x)$. Because α is a cyclic generator of the multiplicative group $G = GF(2^n) = \{\alpha^k | 0 \leq k < |G|\}$, then for every α^i in G, there exists a unique α^j, where $i < j$ that satisfies the above relation. The difficulty of the problem is finding a computationally feasible algorithm that finds j in terms of i, without generating the entire field. One method is to compute Zech's logarithm table for $GF(2^n)$ [3], also referred to as a table of Shift-and-Add (SAA) pairs [4].

If we have a primitive polynomial of degree n over $GF(2)$ with only three terms, then the polynomial itself defines an entry in the SAA table. The occurrence of primitive trinomials for an arbitrary degree n is infrequent but a great amount of research exists on primitive trinomials [5, 6, 7]. Primitive pentanomials are more pervasive than primitive trinomials. Thus we investigate pentanomials and higher term polynomials of the form $f(x) = x^n + p(x)$, where $p(x)$ is a row of Pascal's triangle modulo two. The motivation for requiring that $p(x)$ be a row of Pascal's triangle is that for such polynomials, $p(x) = (x+1)^k$, where k is the particular row of Pascal's triangle with the coefficients taken modulo two. So we can rewrite $f(x)$ as $x^n + (x+1)^k$, which appears to provide a possible SAA pair. As an example, consider the primitive polynomial $f(x) = x^7 + x^3 + x^2 + x + 1$ of degree 7 over $GF(2)$ with root α. We can rewrite the equation in the desired form $f(x) = x^7 + (x+1)^3$. If $f(x)$ is primitive, which in this case we know to be true, then we can manipulate the equation using the fact that $\alpha^{2^7-1} = \alpha^0 = 1$, which follows from the fact that α is a cyclic generator of the multiplicative group with a period of $2^7 - 1 = 127$. So if we can find $a \equiv 3^{-1} \pmod{127}$, then we would find the first SAA pair. Since $3^{-1} \equiv 85 \pmod{127}$, we find the solution to the SAA pair by

$$(\alpha + 1)^{3\times 3^{-1}} = \alpha^{7\times 3^{-1} \pmod{127}}$$
$$\alpha + 1 = \alpha^{7\times 85 \pmod{127}} = \alpha^{87}$$

Thus $(1, 87)$ is a SAA pair that corresponds to the exponents $\alpha^0 + \alpha^1 = \alpha^{87}$, and $f(x)$ divides the polynomial $x^{87} + x + 1$. This provides a step toward a solution to a specific DLP in the field $GF(2^n)$ characterized by the specific polynomial $f(x)$.

This thesis investigates properties of polynomials of the form $f(x) = x^n + p(x)$. We define minimal conditions that the polynomial must satisfy if it is to be primitive. We also define these polynomials as row k Pascal polynomials, where k is the corresponding row of Pascal's triangle. Chapter II provides the necessary background in Number Theory, Group Theory, Field Theory, and Galois Theory. The reader versed in these areas may wish to skip directly to the problem statement beginning in Chapter III.

II. BACKGROUND AND REVIEW

Before beginning a discussion of the problem we investigate, we present some basic definitions and theorems. This information is available in any standard algebra text, such as Beachy and Blair's *Abstract Algebra* [8], or number theory text, such as Rosen's *Elementary Number Theory* [9]. When discussing groups and fields, it should be understood that this paper is only concerned with finite fields. It is also assumed that the reader is familiar with common mathematical, logical, and set notation.

A. NUMBER THEORY

An integer a is called a ***multiple*** of a non-negative integer b if $a = bq$ for some integer q. We also say that b is a ***divisor***, or ***factor*** of a denoted by $b|a$ [8]. Given two integers a and b, not both 0, there exists a positive integer d such that: (i) d is a divisor of both a and b, and (ii) any divisor of both a and b is also a divisor of d. This ***greatest common divisor*** of a and b is denoted by $\gcd(a, b)$ or simply (a, b). If $(a, b) = 1$, then a and b are said to be ***relatively prime***. If p is a prime number then $(a, p) = 1$ for all positive integers a less than p [8, 9].

With the notion of divisibility, it is useful to define a relationship among integers with equal remainders when divided by an integer n. For any positive integer n, the integers a and b are ***congruent modulo n*** if they have the same remainder when divided by n. Congruence is denoted by writing $a \equiv b \pmod{n}$. An immediate consequence of this definition is that two integers a and b are congruent modulo n if and only if n divides their difference $a - b$, denoted $n|(a - b) \iff a \equiv b(\bmod n)$ [8, 9]. Also, if n divides a then a is congruent to zero modulo n.

Every integer has at least two factors, itself and one. If an integer is prime, then these are its only factors. If an integer has factors other than itself and one, then we can further decompose these factors into smaller factors until we have a prime factorization of the integer. ***The Fundamental Theorem of Arithmetic*** states that every integer is uniquely expressible as a product of its prime factors. Given a positive integer n, let the prime factorization of n be denoted by

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Euler's Totient Function, commonly referred to as ***Euler's Phi Function*** [8, 9] gives the number of integers less than or equal to n which are relatively prime to n, and is denoted by

$$\phi(n) = n\prod_{i=1}^{k}\left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^{k}\left(p_i^{\alpha_i} - p_i^{\alpha_i - 1}\right).$$

Euler's Theorem provides a useful relationship between the congruences of an integer n and the Phi Function. If a and n are integers relatively prime to each other, then $a^{\phi(n)} \equiv 1 \pmod{n}$ [8, 9]. A corollary to Euler's Theorem provides a simple proof of ***Fermat's Little Theorem***. If p is a prime, then for any integer a relatively prime to p,

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p}, \\ a^{p-1} - 1 &\equiv 0 \pmod{p} \\ a^{p} &\equiv a \pmod{p}, \text{ even if } a = 0. \end{aligned}$$

This last congruence holds even if $(a, p) = p$ [8, 9]. Since this thesis investigates the properties of polynomials based upon Pascal's triangle, we now define how Pascal's triangle is derived from the next few definitions and identities. Given two non-negative integers n and i, the ***binomial coefficient*** $\binom{n}{i}$ (read "n choose i") is defined by

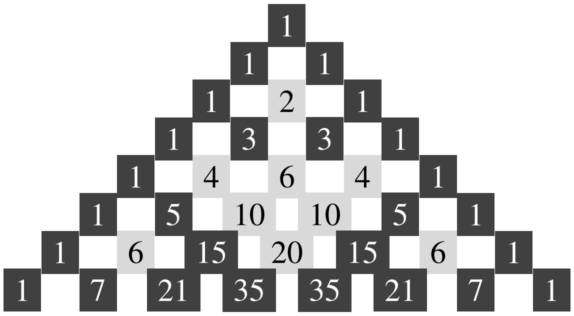
$$\binom{n}{i} = \frac{n!}{i!(n-i)!},$$

for all i such that $0 \leq i \leq n$. Otherwise $\binom{n}{i}$ is equal to zero [9]. ***Pascal's Identity*** defines a recurrence between binomial coefficients. Let n and i be positive integers with $n \geq i$, then

$$\binom{n}{i} = \binom{n-1}{i} + \binom{n-1}{i-1} \quad [9].$$

The ***Pascal triangle*** is a table of the binomial coefficients where $\binom{n}{i}$ is the $(i+1)^{st}$ number in the $(n+1)^{st}$ row. The first eight rows of Pascal's triangle are listed in Figure 1 [9].

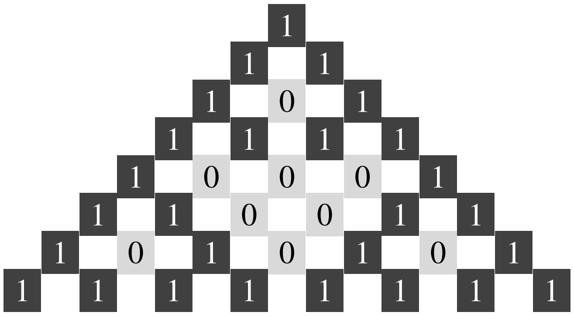
Note that the exterior numbers in the triangle are all ones and the number of terms in each row is equal to one more than the row number. To find an interior number, simply add the two numbers in the positions above and to the left and right of the position being filled (as in the shaded figure above). By Pascal's Identity, this yields the appropriate integer [9].



1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1
1 6 15 20 15 6 1
1 7 21 35 35 21 7 1

Figure 1. Pascal's triangle

Later we want to observe the rows of Pascal's triangle modulo two. Figure 2 shows the coefficients reduced modulo two.



1
1 1
1 0 1
1 1 1 1
1 0 0 0 1
1 1 0 0 1 1
1 0 1 0 1 0 1
1 1 1 1 1 1 1 1

Figure 2. Pascal's triangle modulo two

Again, the exterior numbers in the triangle are all 1 and the number of terms in each row equal one more than the row number. To find an interior number, again add the two numbers in the positions above and to the left and right of the position being filled reducing the sum modulo two. Otherwise, we could compute the standard Pascal triangle and reduce each of the entries modulo two when we arrive at the desired row. Considering memory and computational requirements, the second method is not as efficient as the first where reduction is performed at each row. In fact the *Exclusive OR* operation replaces the addition and reduction modulo two with one logical gate.

Pascal's Identity and Pascal's triangle combine to form the ***Binomial Theorem*** for polynomials. We provide a short combinatorial proof of the Binomial Theorem. The inductive proof can be found in Rosen's *Number Theory* text [9].

Theorem II.1 (Binomial Theorem): *Given two real numbers a and b and any positive integer n, then*

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$$

Proof (Binomial Theorem). Consider how to get a term of the form $a^{n-i}b^i$ from the product of n terms of the form $(a+b)$:

$$(a+b)^n = (a+b)(a+b)\cdots(a+b).$$

We could choose the b's from any i number of the n factors. There are $(n-i)$ factors remaining to choose the a's from. The number of ways to choose i objects from a collection of n objects without replacement, where order is not important, is simply $\binom{n}{i}$. Thus, each $a^{n-i}b^i$ term has coefficient $\binom{n}{i}$, which completes the proof. □

B. GROUP THEORY

A ***group*** is defined as a set of elements G with an associated binary operation $*$ on the elements of G and is denoted by $[G, *]$. However, we will abuse this notation by writing G to indicate the group, only if the operation is understood from the context. The group satisfies the following conditions [8]:

Closure: For all $a, b \in G$, $a * b = c$ for some $c \in G$.

Associativity: For all $a, b, c \in G$, $a * (b * c) = (a * b) * c$.

Identity: There exists $e \in G$, such that for all $a \in G$, $a * e = e * a = a$.

Inverses: For all $a \in G$, there exists $a^{-1} \in G$,such that $a * a^{-1} = a^{-1} * a = e$.

Furthermore, because the groups we are investigating are associated with a field, they also satisfy the commutative property and are referred to as ***abelian*** groups [8].

Commutativity: For all $a, b \in G$, $a * b = b * a$.

A group G is said to be a ***finite group*** if the set G has a finite number of elements. In this case, the number of elements is called the ***order*** of G, denoted by $\#G$ or $|G|$ [8].

An example of a group is the set of congruence classes of the integers modulo n under addition modulo n. Given a positive integer n, we denote the ***congruence classes*** by $[a]_n$ which is the set of all integers congruent to a modulo n. The set of congruence classes of n is denoted by

$$\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-2]_n, [n-1]_n\}$$

This set forms a group under addition where $[a]_n + [b]_n = [a+b]_n$ and is denoted $G_n = [G_n, +]$ [8].

Let G be a group and a be any element of G, then the set $\langle a \rangle = \{x \in G | \, x = a^i, \text{for all } i \in \mathbb{Z}\}$ is called the ***cyclic subgroup generated by a***. The group G is called a ***cyclic group*** if there exists an element a in G such that $G = \langle a \rangle$. In this case a is called a ***generator*** of G and the successive powers of a generate every element of the group [8]. Furthermore, if n is a prime p, then the set $G_p^* = G_p - \{[0]_p\}$ forms a group under multiplication modulo n. Note the necessary requirement to remove the zero class because zero has no inverse under multiplication. An important characteristic of the integers modulo a prime p is that every such group is a cyclic group. If $p > 2$, then the group has at least two generators.

C. FIELD THEORY

A ***field*** is a set of elements F together with the two binary operations $+$ and $*$ on F and is denoted by $F = [F, +, *]$. A field satisfies the following conditions [8]:

Addition: The set F is an abelian group under addition with identity zero.

Multiplication: The set $F - \{0\}$ is an abelian group under multiplication with nonzero identity one.

Distributive: For all $a, b, c \in F$, $a * (b + c) = (a * b) + (a * c)$.

If the set F is finite, then the field F is a ***finite field***. If F is a finite field, the multiplicative group is cyclic. Since it forms the foundation as the base field for our further discussion, we now provide the operation tables for the integers modulo two, also called the Galois Field of two elements, as an example.

$+$	0	1
0	0	1
1	1	0

Table II.1 Addition in $GF(2)$

$*$	0	1
0	0	0
1	0	1

Table II.2 Multiplication in $GF(2)$

The next section describes Galois Fields in greater detail, but we provide a quick definition here to clarify our notation. A Galois Field is any finite field with a prime, or a power of a prime, order. Galois Field's are denoted in several ways, to include the following notations; $GF(p^n)$, $\mathbb{F}_{p^n}$, and $GF(p)[x]/\langle f(x) \rangle$ (where f is a polynomial that generates the field, which we further explain in the following section) are the most common notations.

We predominantly use the first notation throughout this paper. Therefore, $GF(2)$ is the field with only two elements, namely $\{0, 1\}$. Thus, $GF(2^n)$ is the polynomial field whose variable coefficients are contained in the subfield $GF(2)$. We now provide more rigorous definitions of these terms.

Let F be a field. If $a_n, a_{n-1}, \ldots, a_1, a_0 \in F$ (where n is a non-negative integer), then any expression of the form $a_n x^n + a_{n-1} x^{x-1} + \cdots + a_1 x + a_0$ is called a ***polynomial over F*** in the ***indeterminate x*** with coefficients $a_n, a_{n-1}, \ldots, a_0$. We also call F the ***base field*** or ***ground field***. The subscript i of the coefficient a_i is called the ***index*** [8]. If n is the largest non-negative index such that $a_n \neq 0$, then we say that the polynomial $f(x) = a_n x^n + \cdots + a_1 x + a_0$ has ***degree n***, written deg$(f(x)) = n$, and a_n is called the ***leading coefficient*** of $f(x)$. If the leading coefficient of $f(x)$ is one, then $f(x)$ is said to be a ***monic polynomial***. The set of all polynomials with coefficients in F is denoted by $F[x]$ [8]. An element c is called a ***root*** of $f(x)$ if $f(c) = 0$ [8]. While it is possible for a polynomial to have a root in its base field F, it is not necessary. In fact $f(x)$ may have no roots in its base field. In this case, all of the roots of $f(x)$ exist in some extension field which we define shortly.

Similar to the division algorithm for the integers, we can define a division algorithm for polynomials. For any polynomials $f(x)$ and $g(x)$ in $F[x]$, with $g(x) \neq 0$, there exist unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = q(x)g(x) + r(x)$ where either deg$(r(x)) <$ deg$(g(x))$ or $r(x) = 0$ (See [8] p.163 for a proof). Just as the division algorithm in $\mathbb{N}$ has a polynomial counterpart, so does the concept of congruences. Let F be a field, and $p(x)$ be a fixed polynomial over F. If $a(x), b(x) \in F$, then we say that $a(x)$ and $b(x)$ are ***congruent modulo p(x)***, written $a(x) \equiv b(x) \pmod{p(x)}$, if $p(x)|(a(x) - b(x))$. The set $\{b(x) \in F[x] | a(x) \equiv b(x) \pmod{p(x)}\}$ is called the ***congruence class*** of $a(x)$, and is denoted by $[a(x)]_{p(x)}$. The set of all congruence classes modulo $p(x)$ is denoted by $F[x]/\langle p(x) \rangle$ [8].

A non-constant polynomial is said to be ***irreducible*** over the field F if it cannot be factored in $F[x]$ into a product of polynomials of only lower degree. It is said to be reducible over F if such a factorization exists [8]. The base field F of a polynomial field $F[x]$ can be either an infinite or finite field. Throughout this thesis we consider the base field $GF(2)$. As an example of reducibility, we define the polynomials $f_1(x), f_2(x), g_1(x), g_2(x) \in F[x]$, where $f_1(x) = x^2 + 1$, $f_2(x) = x^2 + x + 1$, $g_1(x) = x$, $g_2(x) = x + 1$. Note that $f_1(x)$ has the factorization $x^2 + 1 = (x + 1)(x + 1) = (x + 1)^2 = (g_2(x))^2$, and so $f(x)$ is reducible. But since $g_1(x)$ and $g_2(x)$ (which are the only degree one polynomials in $GF(2)$) do not divide $f_2(x)$ exactly, $f_2(x)$ is irreducible. By the ***Fundamental Theorem of Algebra***, every polynomial of degree n has n roots. If all of the factors of a polynomial are not linear over the base field, then its roots must exist in some larger field. This suggests the concept of an extension field, but first we provide a familiar example.

The polynomial $x^2 + 1$ has no roots in the field $\mathbb{R}$ of real numbers. However, we obtain a root by introducing the element i for which $i^2 = -1$ and adjoining it to the field $\mathbb{R}$. This leads to the definition of the field of complex numbers, denoted by $\mathbb{C}$, which contains elements of the form $\alpha + i\beta$, where α and β are elements of $\mathbb{R}$. In a similar manner, we can construct larger fields in which any polynomial, over any field, has a root. To accomplish this we use congruence classes of polynomials [8]. Let E and F be fields. If F is a subset of E and is closed under the operations of addition and multiplication defined for E, then F is called a ***subfield*** of E, and E is called an ***extension field*** of F [8]. Let F be an extension field of the field K. If the dimension of F as a vector space over K is finite, then F is said to be a ***finite extension*** of K [8].

Let K be a field and let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial in $K[x]$ irreducible over K. If F is an extension field of K, then F is a ***splitting field*** for $f(x)$ over K if there exist elements $r_1, r_2, \ldots, r_n$ in F such that $f(x) = a_n(x - r_1)(x - r_2)\ldots(x - r_n)$, and $F = K(r_1, r_2, \ldots, r_n)$. The elements $r_1, r_2, \ldots, r_n$ are roots of $f(x)$, and so F is obtained by adjoining to K a complete set of the roots of $f(x)$. We say that $f(x)$ ***splits*** over the field E if E contains the splitting field of F [8].

D. GALOIS THEORY

We now have the necessary definitions and theorems to define a Galois field. If p is any prime and k is any integer, there exists a unique finite field of order p^k. This field is called the ***Galois field*** of order p^k and is denoted by $GF(p^k)$ [8]. The ***characteristic*** of a Galois field is defined by the order of the base field, namely p. Because of its applications in electronic data systems, we are interested in Galois fields of characteristic two denoted by $GF(2)$.

Given an irreducible polynomial $f(x)$ of degree n over $GF(2)$ with the complex root α, then α is a ***primitive element*** of $f(x)$ if and only if α is a multiplicative generator of all nonzero elements of $GF(2^n)$. Moreover, $f(x)$ is defined to be a ***primitive polynomial*** if $f(x)$ has an associated root α which is a primitive element. Then the powers of α^i, where

$i \in \{0, 1, 2, \ldots, 2^n - 2\}$, are all distinct elements when reduced modulo $f(x)$ and modulo two. The set of elements generated by $f(x)$ is defined as $GF(2^n) = \frac{GF(2)[x]}{\langle f(x) \rangle} = \{\alpha^i | i \in \mathbb{Z}^+_{2^n-1}\}$, where $n = \deg(f(x))$. These elements comprise the splitting field of $f(x)$ over $GF(2^n)$, where addition and multiplication are well defined.

Although the primitive element α is a multiplicative generator for $GF(2^n)$, α does not provide a relationship of the elements under addition. Our motivation for this thesis is to search for polynomials that provide insight into the relationship between addition and multiplication in certain representations of $GF(2^n)$. The additive properties of each α^i is fundamentally the Discrete Logarithm Problem as presented in Chapter I.

If a polynomial of degree n is primitive, that polynomial is said to generate all the nonzero elements of the field. However each element α^i in $GF(2^n)$ is uniquely expressible as a linear combination of elements of the set $P = \{\alpha^0, \alpha^1, \alpha^2, \alpha^3, \ldots \alpha^{n-1}\}$, where P is referred to as a ***polynomial basis*** of $GF(2^n)$. That is to say, if we consider only the coefficients of an element of $GF(2^n)$, we can represent the coefficients as a vector of length n. For example, if a primitive polynomial has degree three, the element $x^j = x^2 + x$ is annotated as the vector $[\,1 \quad 1 \quad 0\,]$ and the element $x^k = x + 1$ is associated to the vector $[\,0 \quad 1 \quad 1\,]$. So a primitive polynomial of degree three generates all possible binary 3-long vectors, or 3-tuples, except for the all zeros vector. Since the entries in the vector are either zero or one, as defined by the base field $GF(2)$, there are $2^n - 1$ nonzero elements in the field.

i	x^2	x	1
0	0	0	1
1	0	1	0
2	1	0	0
3	0	1	1
4	1	1	0
5	1	1	1
6	1	0	1

Table II.3 Multiplicative group generated by $f(x) = x^3 + x + 1$

Consider the primitive polynomial $f(x) = x^3 + x + 1$ over $GF(2)$. This polynomial has no roots in the base field , but the adjoined root α in the extension field gives $f(\alpha) = \alpha^3 + \alpha + 1 = 0$. Subsequent powers of α generate all possible 3-tuples in an order determined modulo the polynomial and the coefficients modulo two. Without loss of generality, we shall express the elements of the field using the indeterminate variable x

rather than the root α. Table II.3 lists the nonzero elements of the field generated as powers of α represented by $x^i = a_2x^2 + a_1x + a_0$. The first column, i, is the power of the generator, while the remaining columns represent the coefficient vector described above.

Recall that a primitive polynomial with a multiplicative generator creates the multiplicative group of all $2^n - 1$ nonzero elements. So the ***period*** of a primitive polynomial is $2^n - 1$. If a polynomial of degree n is irreducible but not primitive, then its period is some divisor of $2^n - 1$. Since α is a primitive root of $f(x)$ of degree n, every element of $GF(2^n)$ can be represented as linear combinations of the first n powers of α. The representation of each element is uniquely determined by $f(x)$, as in Table II.3, and the zero element is represented as the all 0 vector.

The first well known property of Galois Fields is the ***characteristic identity***, as defined in the following theorem.

Theorem II.2: *Given a polynomial $f(x)$ over $GF(p)$, then $(f(x))^{p^k} = f(x^{p^k})$, which is defined as the characteristic identity of a finite field.*

Proof. We write the function $f(x)$ as $\sum_{i=0}^{n} a_i x^i = a_n x^n + \sum_{i=0}^{n-1} a_i x^i = a_n x^n + g_1(x)$. It follows from the Binomial Theorem that

$$\begin{aligned}(f(x))^{p^k} &= (a_n x^n + g_1(x))^{p^k} \\ &= \sum_{i=0}^{p^k} \binom{p^k}{i} \left(a_i x^i\right)^{p^k - i} (g_1(x))^i\end{aligned}$$

But $\binom{p^k}{i} = \frac{p^k!}{i!(p^k-i)!} \equiv 0 \pmod{p}$ for all i except zero and p^k. So the above expression reduces to $(a_n x^n)^{p^k} + (g_1(x))^{p^k} = (a_n)^{p^k} \left(x^{p^k}\right)^n + (g_1(x))^{p^k}$. By Fermat's Little Theorem, $(a_n)^{p^k} \equiv a_n \pmod{p}$. We repeat this process for each successive term until $g_{n-1}(x) = a_1 x + a_0$. By the same procedure as above, $(g_{n-1}(x))^{p^k} = (a_1 x + a_0)^{p^k} = a_1(x^{p^k}) + a_o$. Thus $(f(x))^{p^k} = \sum_{i=0}^{n} a_i \left(x^{p^k}\right)^i = f(x^{p^k})$, which completes the proof. □

There are two well known results regarding the number of primitive and irreducible polynomials of degree n over a finite field. The number of primitive polynomials of degree n is given by

$$\#P_n = \frac{\phi(2^n - 1)}{n},$$

where $\phi(n)$ is the totient function, and the number of irreducible polynomials is

$$\#I_n = \frac{1}{n}\sum_{d|n} \mu(d)2^{n/d},$$

where μ is the Möbius function. Also note, that if $f(x)$ is a primitive or irreducible polynomial over $GF(2)$, so too is the reciprocal polynomial $f^*(x) = x^n \cdot f(\frac{1}{x})$, where n is the degree of $f(x)$.

Theorem II.3: *If* $f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0$ *is a primitive polynomial over* $GF(2)$*, then* $f^*(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-2}x^2 + a_{n-1}x + a_n$ *is also a primitive polynomial.*

Proof. It is sufficient to show a mapping from $f(x)$ to $f^*(x)$. We show that $f^*(x) = x^n \cdot f(\frac{1}{x})$.

$$\begin{aligned}
f\left(\frac{1}{x}\right) &= a_n\left(\frac{1}{x}\right)^n + a_{n-1}\left(\frac{1}{x}\right)^{n-1} + \cdots + a_2\left(\frac{1}{x}\right)^2 + a_1\left(\frac{1}{x}\right)^1 + a_0\left(\frac{1}{x}\right)^0 \\
x^n \cdot f\left(\frac{1}{x}\right) &= x^n\left[a_n\left(\frac{1}{x}\right)^n + a_{n-1}\left(\frac{1}{x}\right)^{n-1} + \cdots + a_2\left(\frac{1}{x}\right)^2 + a_1\left(\frac{1}{x}\right)^1 + a_0\left(\frac{1}{x}\right)^0\right] \\
&= a_nx^0 + a_{n-1}x^1 + \cdots + a_2x^{n-2} + a_1x^{n-1} + a_0x^n \\
&= a_0x^n + a_1x^{n-1} + \cdots + a_{n-2}x^2 + a_{n-1}x + a_n = f^*(x)
\end{aligned}$$

Since $x^n \cdot f(\frac{1}{x}) = f^*(x)$, $f^*(x)$ is also a primitive polynomial, which completes the proof. □

Consider the example of $f(x) = x^7 + x^3 + x^2 + x + 1$. Since this polynomial is primitive over $GF(2)$, so is $x^7 \cdot f(\frac{1}{x}) = x^7 + x^6 + x^5 + x^4 + 1$. So if we find one primitive polynomial, we have actually found two. This simplifies our search for Pascal polynomials since we need only test half as many polynomials.

E. TESTS FOR IRREDUCIBILITY/PRIMITIVITY

There are primarily two methods to test a polynomial for irreducibility and two methods for testing primitivity. The first method for testing irreducibility and primitivity is called the ***sieving method***. This requires a complete listing of all irreducible polynomials whose degree is half of the degree of the polynomial in question. For example, suppose a polynomial $f(x)$ has degree 33. We would require a complete list of irreducible polynomials up to degree $\lfloor \frac{33-1}{2} \rfloor = 16$. To then determine irreducibility, we would successively divide $f(x)$ by each irreducible polynomial in our list. If any polynomial, say $g(x)$, divides $f(x)$ without a remainder, then $f(x)$ is reducible since $\frac{f(x)}{g(x)} = p(x)$ [1]. Once we know a polynomial $f(x)$ to be irreducible, we assume it has an associated primitive root α which is a generator of all $2^n - 1$ nonzero elements. We successively compute the powers of α modulo $f(x)$ modulo two. If α^j repeats any element α^i such that $0 < i < j < 2^n - 1$, then $f(x)$ is imprimitive. Note that as the degree of the polynomial increases, this method is very computationally expensive and therefore very undesirable.

The second method is a nine step algorithm presented by S. E. O'Connor [10] that checks both irreducibility and primitivity of a polynomial over an arbitrary ground field $GF(p)$, where p is prime. This method is preferred due to computational speed and efficiency. However, since we consider only the ground field $GF(2)$, we can omit steps 2 and 6 from the original algorithm. Also, since our polynomials are not randomly generated, we show in the beginning of Chapter 3 that Pascal polynomials have no linear factors over $GF(2)$, and so we omit step 3. Furthermore, we omit the Berlekamp test for irreducibility as the final step will filter out any reducible polynomials that pass Step 2. Our modified algorithm is simplified over $GF(2)$ where we assume there exists an efficient algorithm for factoring $2^n - 1$. Since polynomial division is a simple shift of a bit string combined with a bitwise XOR operation, of which both operations are native to microprocessors, the most difficult step in the algorithm is factoring $2^n - 1$. We now present a modified and renumbered version of the algorithm for testing Pascal polynomials over $GF(2)$.

Step 1: Generate a new degree n monic Pascal polynomial over $GF(2)$ of the form $f(x) = x^n + (x+1)^k$.

Step 2: Check if $x^{2^n-1} \equiv 1 \pmod{(f(x), 2)}$ and reject the polynomial as reducible if the equivalence is not true.

In this step, we note that the cyclotomic polynomial $c(x) = x^{2^n-1} + 1$ contains as its roots all $2^n - 1$ complex roots of unity on the unit circle defined in the complex plane of numbers [1]. Thus any irreducible polynomial $f(x)$ of degree n contains as its roots some subset of the roots of $c(x)$ [1]. Therefore, if $f(x)$ does not divide $c(x)$ without remainder, then $f(x)$ is reducible over $GF(2)$. We must still check that $f(x)$ is not a product of smaller order polynomials that also divide $c(x)$.

Step 3: Factor $r = 2^n - 1$, into distinct primes; $r = p_1^{e_1} \dots p_k^{e_k}$.

Step 4: Check if $x^m \equiv 1 \pmod{(f(x), 2)}$, where $m \in \{\frac{r}{p_1}, \frac{r}{p_2}, \dots, \frac{r}{p_k}\}$, and reject the polynomial as not primitive if any of these equivalences are true.

This step utilizes **Lagrange's Theorem** which states that if S is a subgroup of a group G, then the order of S divides the order of G [8]. So with a complete factorization of r, we continue to divide $f(x)$ into each of the cyclotomic polynomials whose degrees are a combination of the factors of $2^n - 1$. A consequence of Step 4 is that if a polynomial has prime degree p, such that $2^p - 1$ is a ***Mersenne prime***, then all irreducible polynomials of degree p are in fact primitive. Since Mersenne primes are very rare among the Mersenne numbers, it provides us little computational efficiency to rely on this consequence and incorporate individual tests for irreducibility into our algorithm. In the case of randomly generated polynomials, a separate test for irreducibility could provide added speed to the algorithm. However, our polynomials have a noticeable structure and are not randomly generated. We expect to see a large number of these polynomials as primitive and will likely reach the step in O'Connor's algorithm that factors 2^n-1, which is arguably the most difficult step in the algorithm. For a complete explanation of why we can omit Berlekamp's Test for Irreducibility and move right to our Step 4, reference Appendix A.

Step 5: If $f(x)$ passes steps 1 through 4, accept it as primitive.

As an example, consider the previous polynomial $f(x) = x^7 + (x+1)^3 = x^7 + x^3 + x^2 + x + 1$ where $c(x) = x^{127} + 1$. Performing the polynomial division modulo two shows that $f(x)$ divides $c(x)$ without remainder. Since $2^7 - 1 = 127$ is a Mersenne prime, $f(x)$ cannot have period smaller than 127 and is therefore primitive.

So what if $2^n - 1$ is not a Mersenne prime? Consider these three examples of reducible polynomials; $f_1(x) = x^6+x^3+x^2+x+1$, $f_2(x) = x^6+x^5+x^4+x^3+x^2+x+1$, and $f_3(x) = x^6+x^2+1$. Note that f_1 is also a Pascal polynomial where $f_1(x) = x^6+(x+1)^3$. However, f_1, f_2, and f_3 are reducible having the factors $f_1(x) = (x^2+x+1)(x^4+x^3+1)$, $f_2(x) = (x^3+x+1)(x^3+x^2+1)$, and $f_3(x) = (x^3+x+1)^2$(which has repeated factors). Now let's look at the factorization of $c(x) = x^{2^6-1}+1$,

$$\begin{aligned} c(x) =&(x+1)(x^2+x+1)(x^3+x+1)(x^3+x^2+1) \\ &(x^6+x+1)(x^6+x^3+1)(x^6+x^4+x^2+x+1)\cdots \end{aligned}$$

where the remaining factors of $c(x)$ are the remaining irreducible sixth degree polynomials. Note that f_1 will not divide $c(x)$, since $c(x)$ does not have (x^4+x^3+1) as one of its factors. Also note that f_3 will not divide $c(x)$, since $c(x)$ only has (x^3+x+1) as one of its factors once, not twice. Thus f_1 and f_3 would have been eliminated in Step 2. Now f_2 is a little tricky since $c(x)$ has as its factors both of the factors of f_2. So f_2 will pass Step 2 since it evenly divides $c(x)$, but it will not pass Step 4. Both factors of f_2 are themselves primitive polynomials with period $2^3 - 1 = 7$. The period of f_2 is therefore the period of the least common multiple of the periods of its factors. So the period of f_2 is seven. Step 3 shows the factors of $2^6 - 1 = 63 = 3^2 \cdot 7$. When we divide $x^{3 \cdot 7} + 1 = x^{21} + 1$ by f_2, the remainder will be zero and we reject this polynomial as primitive.

F. LINEAR-FEEDBACK SHIFT REGISTERS

A Linear-Feedback Shift Register, or LFSR, is an electronic hardware or software representation of a polynomial over $GF(2)$. A LFSR is a finite-state machine whose successive states are uniquely determined by the previous state of the register. We denote a state by s_i and define a function $\gamma(s_i)$ to be the operation performed by the register where $s_{i+1} = \gamma(s_i)$ [1]. Each successive state corresponds to a time-step of the register where the output of the register at each time-step is a single bit. A LFSR is equivalent to a polynomial over $GF(2)$ such that $\gamma(s_i) = \sum_{k=0}^{n-1} a_k x^k = f(x)$ where the a_i's are the coefficients of the terms with degree less than n of the polynomial $f(x)$. If a primitive polynomial is used to represent the operation of the register, then the resulting sequence of outputs is an m-sequence of full length or period. As expected, a full-length m-sequence has period $2^n - 1$ where n is the degree of the primitive polynomial represented by the register.

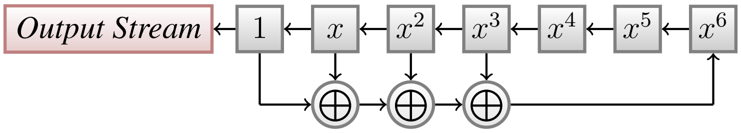


Figure 3. Fibonacci LFSR for $f(x) = x^7 + x^3 + x^2 + x + 1$

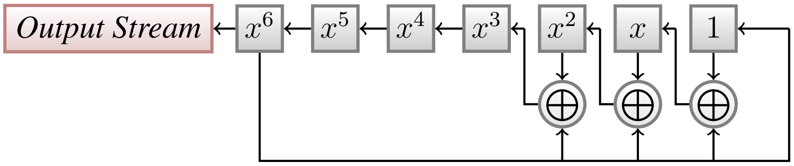


Figure 4. Galois LFSR for $f(x) = x^7 + x^3 + x^2 + x + 1$

There are essentially two classical types of LFSRs, the Fibonacci register and the Galois register. The Galois register is useful for generating the successive powers of the primitive element α and the state of the machine at time i gives the field representation of α^i. Table II.3 is the actual output of the Galois register represented by the primitive polynomial $f(x) = x^3 + x + 1$. While the bit-stream output from both registers is identical at certain offsets, the Fibonacci register is computationally more efficient at producing the m-sequence without regard to the field representation of $f(x)$. Figure 3 and Figure 4 demonstrate the operation of the two registers given the primitive polynomial $f(x) = x^7 + x^3 + x^2 + x + 1$.

For the primitive polynomial $f(x) = x^3+x+1$, the m-sequence output is $[\,0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 1 \quad 1\,]$. If we take a linear shift of the m-sequence by some number of bits i and sum the bits of the shifted sequence to the original sequence modulo two, the result is the same sequence shifted by a number of bits j. First, a labeling of the m-sequence is necessary to determine the magnitude of the shift. We label each sequence in the following fashion,

$$\begin{array}{ccccccc} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ S_0 & S_1 & S_2 & S_3 & S_4 & S_5 & S_6 \end{array}$$

We next take the original sequence with a shift of one, and add each bit modulo two as follows.

$$\begin{array}{ccccccc} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ \hline 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{array} \qquad \begin{array}{ccccccc} S_0 & S_1 & S_2 & S_3 & S_4 & S_5 & S_6 \\ S_1 & S_2 & S_3 & S_4 & S_5 & S_6 & S_0 \\ \hline S_3 & S_4 & S_5 & S_6 & S_0 & S_1 & S_2 \end{array}$$

The resulting sequence is a shift of the original sequence by 3 positions.

Shift-and-Add (SAA) pairs [4], also referred to as Cycle-and-Add pairs [1], are only defined for primitive polynomials and therefore allow for a method for performing addition within a respective field as characterized by a primitive polynomial $f(x)$. In particular, SAA pairs describe two elements of the field whose sum, taken modulo two, differs only by $x^0 = 1$. Observe from Table II.3 that $x^2 + x^6 = 1$. So x^2 and x^6 are also SAA pairs and we denote this relationship by writing the exponents as an ordered pair. Thus $(1, 3)$, $(2, 6)$, and $(4, 5)$ are examples of SAA pairs as seen in Table II.3. In the example of $f(x) = x^3 + x + 1$, we notice that $f(x)$ is a trinomial. Primitive trinomials are desirable in that they give an immediate SAA pair for the field. By setting a primitive trinomial $f(x)$ equal to zero, we get the first SAA pair by

$$\begin{aligned} x^3 + x + 1 &= 0 \\ x^3 &= x + 1. \end{aligned}$$

Squaring both sides of the equation gives $x^6 = (x+1)^2$. By the Binomial Theorem, $(x+1)^2 = x^2 + 2x + 1$. Reducing the coefficients modulo two, $(x+1)^2 = x^2 + 1$ and thus $x^6 = x^2 + 1$. Squaring once more gives $x^{12} = x^5 = (x^2+1)^2 = x^4 + 1$. Thus, from one SAA pair we can generate a table that defines addition within the field. If we wanted to know the sum, $x^3 + x^4$, as a power of the primitive element, we simply perform the following reduction

$$\begin{aligned} x^3 + x^4 &= x^3(x+1) \\ &= x^3x^3 = x^{3+3} \\ &= x^6 = x^2 + 1. \end{aligned}$$

Thus the SAA or Zech's Logarithm table, provides a convenient method of performing addition within $GF(2^n)$ without computing the entire multiplication and addition tables for $f(x)$. Note that as the degree of the polynomial increases, the size of the field grows exponentially. However, the "squaring method" of finding SAA pairs only provides a linear growth in the number of SAA pairs immediately obtainable. Some work is required to compute the rest of the SAA table, but efficient algorithms provide a method of completing this table. Since every primitive polynomial divides the polynomial representations of each of its SAA pairs, we can search for the next SAA pair not in our table by computing $\frac{1+x^i}{f(x)} + r = x^j$. The singleton remainder term x^j gives the SAA pair (i, j).

Consider the polynomial $f(x) = x^7 + x^3 + x^2 + x + 1 = x^7 + (x+1)^3$, we know from Chapter 1 that the first SAA pair for this polynomial is (1,87). Recall that this SAA pair corresponds to the trinomial $x^{87} + x + 1$. Squaring the trinomial gives $x^{174} + x^2 + 1$. Reducing the exponents modulo 127 gives the trinomial $x^{47} + x^2 + 1$, resulting in the SAA pair (2,47). So we get the first seven SAA pairs by taking $(2^k \times 1, 2^k \times 87) \pmod{127}$ where $0 \leq k \leq n-1$. The first seven SAA pairs for $f(x)$ are $(1, 87)$, $(2, 47)$, $(4, 94)$, $(8, 61)$, $(16, 122)$, $(32, 117)$, and$(64, 107)$. We get seven more SAA pairs by multiplying the original trinomial $x^{87} + x + 1$ by x^{-1}, and performing the squaring operation again by taking $(2^k \times (-1), 2^k \times (87-1)) \pmod{127}$. The resulting SAA pairs are $(126, 86)$,

$(125, 45)$, $(123, 90)$, $(119, 53)$, $(111, 106)$, $(95, 85)$, and$(63, 43)$. Again, we get seven more by multiplying by x^{-87} and taking $(2^k \times (-87), 2^k \times (1-87)) \pmod{127}$. This time, the resulting SAA pairs are $(40, 41)$, $(80, 82)$, $(33, 37)$, $(66, 74)$, $(5, 21)$, $(10, 42)$, and$(20, 84)$.

The first 63 SAA pairs were relatively straightforward to find, but there are still 63 more to be found. The first integer that is not in a SAA pair is 3. To find the j that satisfies $x^j + x^3 + 1$, we multiply $x^3 + 1$ by x^{127}. We begin reducing $x^{130} + x^{127}$ by adding multiples of $f(x)$ modulo two. Clearly $x^{2^n-1} \equiv 1 \pmod{(f(x), 2)}$, for any primitive polynomial $f(x)$ with degree n, so dividing by $f(x)$ will simply return what we began with. But while performing the polynomial division, there is a polynomial multiple of $f(x)$ that when added to $x^{130} + x^{127}$, leaves a single remainder term. This singleton remainder results in the desired j that we were looking for. In this case the SAA pair is thus (3,57). We can perform the squaring and multiplying procedure to find the next 21 SAA pairs.

III. PASCAL POLYNOMIALS

We continue by considering polynomials of the form $f(x) = x^n + p(x)$, where $p(x)$ is a row of Pascal's triangle modulo two. We define polynomials of this form as ***Pascal polynomials***. Since each row of Pascal's triangle can be viewed as the coefficients in the expansion of $(x + 1)^k$, any polynomial that can be represented in the form of a row of Pascal's triangle plus an additional monomial term *resembles* a trinomial. It would be very nice to find a primitive polynomial of this form because we could then find an easy solution for the first SAA pair.

Why do we care if $p(x)$ is a row of Pascal's triangle? The most obvious reason, as stated above, is that a Pascal polynomial of the form $f(x) = x^n + (x + 1)^k$ is similar to a trinomial of the form $g(x) = x^n + x^k + 1$. The not so obvious reason to choose polynomials of this form is that when $f(x) = x^n + (x + 1)^k$, $f(x)$ has no linear factors. This allows us to exclude Step 3 in O'Connor's test for irreducibility/primitivity. Any row of Pascal's triangle modulo two has an even number of nonzero terms, with the outermost terms always being 1. Thus adding the additional x^n term yields a polynomial with an odd number of terms, and $f(x)$ has no solutions in the ground field $GF(2)$.

Theorem III.1: *Any polynomial of the form $f(x) = x^n + (x + 1)^k$ has no linear factors over $GF(2)$, where $n > 0$ and $k > 0$.*

Proof. Evaluating $f(x)$ over the ground field, we see that

$$f(0) = 0^n + (0 + 1)^k = 0 + (1)^k \equiv 1 \pmod{2}, \text{ and}$$
$$f(1) = 1^n + (1 + 1)^k = 1 + (2)^k \equiv 1 \pmod{2}.$$

So $f(x)$ has no linear factors, which completes the proof. □

Since we have just shown that polynomials of the form $f(x) = x^n + (x + 1)^k$ have no linear factors over the ground field, we can exclude this step in our test for irreducibility. This thesis investigates some specific cases of the generalized class of polynomials over $GF(2)$ of the form $f(x) = x^n + (x^a + 1)^k$. For now we set $a = 1$, giving polynomials of the form $f(x) = x^n + (x + 1)^k$. Recall that the fewer terms in a primitive polynomial, the fewer addition operations, and the faster we can implement the algorithm in hardware/software. So a polynomial with fewer terms is presumably more computationally efficient when wired up as an LFSR, thus trinomials are preferred over pentanomials which are preferred over heptanomials, etc... It would be nice to know which rows of Pascal's triangle will yield four terms, six terms, eight terms, etc... Consider the following theorem.

Theorem III.2: *The number of odd terms in row k of Pascal's triangle is $2^{\mathrm{wt}(k)}$, where* wt (k) *is the Hamming weight of k and represents the number of one's in the binary expansion of k.*

Proof. Let $f(x) = (x+1)^k = \sum_{i=0}^{k} \binom{k}{i} x^i$ be the polynomial representation of the k^{th} row in Pascal's triangle modulo two. Further, if the Hamming weight of k is $\mathrm{wt}\,(k) = w$, we can write the binary representation of k as $k = \sum_{i=0}^{w} 2^{k_i}$, where $k_1 < k_2 < \cdots < k_w$. Then,

$$\begin{aligned}(x+1)^{\sum_{i=0}^{w} 2^i} &= \prod_{i=0}^{w} (x+1)^{2^i} \\ &= \prod_{i=0}^{w} (x^{2^i} + 1)\end{aligned}$$

by Theorem II.2. It is straightforward to show that any polynomial with n terms will have twice as many terms when multiplied by the binomial $(x^a + 1)$, such that a does not equal any exponent in the original polynomial. Since our last equation has w binomial products, there are 2^w number of terms in the expanded product. The resulting expanded polynomial must match the number of terms in the binomial expansion. So there must be 2^w number of binomial coefficients $\binom{k}{i}$, which are odd. This completes the proof. □

We now know that if k is a power of two, then by Theorem II.2, the polynomial $f(x) = x^n + (x+1)^k = x^n + x^k + 1$. A great deal is known about trinomials over $GF(2)$, thanks to the celebrated Swan's Theorem [5], so we focus the scope of this thesis to polynomials with more than three terms, namely $k \neq 2^t$. But Theorem III.2 shows that our Pascal polynomial yields a pentanomial if and only if the Hamming weight is two.

Corollary III.3: *The polynomial $f(x) = x^n + (x+1)^k$, with $n > k$, is a pentanomial if and only if the Hamming weight of k is 2.*

Proof. Consider $k = 2^s + 2^t$, where $t > s$. Then,

$$\begin{aligned}x^n + (x+1)^{2^t + 2^s} &= x^n + (x+1)^{2^t}(x+1)^{2^s} \\ &= x^n + x^k + x^{2^t} + x^{2^s} + 1\end{aligned}$$

The reciprocal is trivial as the number of terms in $(x+1)^k$ is $2^{\mathrm{wt}(k)} = 2^2 = 4$, by Theorem III.2. This completes the proof. □

Thus, we should focus our attention on rows of Pascal's triangle that have a Hamming weight of two or more. Since three is the smallest number with Hamming weight two, let us begin our examination with row three Pascal polynomials.

A. ROW THREE POLYNOMIALS

We want to know when the pentanomial $f(x) = x^n + x^3 + x^2 + x + 1$ is primitive for $n > 3$. In order to solve for a SAA pair, we note that if $x^n + (x+1)^3 = 0$, then $x^n = (x+1)^3$. Note that a polynomial has the ***SAA property*** if and only if it is primitive. But having a ***SAA solution*** (i.e. $x + 1 = x^{n/3}$) is not a sufficient condition for primitivity. So when $3|n$, $f(x)$ has a SAA solution. But we show now that $f(x)$ of degree $n = 3\tilde{n}$ is reducible with the factor $g(x) = x^2 + x + 1$, therefore $f(x)$ is imprimitive and does not have the SAA property even though it has a SAA solution.

Theorem III.4: *Any polynomial of the form* $f(x) = x^{3\tilde{n}} + x^3 + x^2 + x + 1$ *is reducible over* $GF(2)$.

Proof (Induction). Let $g(x) = x^2 + x + 1$. Clearly $g(x)|(x^2 + x + 1)$, so it is sufficient to show that $g(x)|(x^{3\tilde{n}} + x^3)$. Reducing the monomial term $x^{3\tilde{n}}$ modulo $g(x)$ modulo 2, we have

$$\begin{aligned} x^{3\tilde{n}} + x^{3\tilde{n}-2}(x^2 + x + 1) + x^{3\tilde{n}-3}(x^2 + x + 1) &\equiv \\ x^{3\tilde{n}} + x^{3\tilde{n}} + x^{3\tilde{n}-1} + x^{3\tilde{n}-2} + x^{3\tilde{n}-1} + x^{3\tilde{n}-2} + x^{3\tilde{n}-3} &\equiv \\ x^{3\tilde{n}-3} &\equiv x^{3(\tilde{n}-1)} \pmod 2. \end{aligned}$$

We can continue this reduction until $x^{3\tilde{n}} \equiv x^3 \pmod{(g(x), 2)}$. Therefore $g(x)|(x^{3\tilde{n}} + x^3)$ and it follows that $g(x)|f(x)$, which completes the proof. □

We next consider polynomials of an even degree where $n = 2\tilde{n}$. It is clear that $3 \nmid 2\tilde{n}$ unless $3|\tilde{n}$. If $f(x)$ is a primitive polynomial, then the root α is a cyclic generator of the multiplicative group with period $2^n - 1$ such that $\alpha^{2^n-1} = \alpha^0 = 1$. Therefore, we can multiply the equation, any number of times, by α^{2^n-1} giving

$$\begin{aligned} (x+1)^3 &= x^{2\tilde{n}} \\ &= x^{2\tilde{n}} x^{t(2^{2\tilde{n}}-1)} \\ &= x^{2\tilde{n}+t(2^{2\tilde{n}}-1)}. \end{aligned}$$

Now the exponent looks more complicated and we must determine its divisibility by three. Before investigating this case, we prove a useful lemma.

Lemma III.5: *If 'a' is an even nonnegative integer, then* 3 *divides* $2^a - 1$*. Otherwise if 'a' is odd, then* 3 *divides* $2^a + 1$.

Proof. Since $2 \equiv -1 \pmod{3}$, then $2^a - 1 \equiv (-1)^a - 1 = 0$ if a is even. Otherwise $2^a + 1 \equiv (-1)^a + 1 = 0$ if a is odd, which completes the proof. □

So when the degree of $f(x)$ is even, we now provide a proof that the exponent $2\tilde{n} + t(2^{2\tilde{n}} - 1)$ is not divisible by three. Thus row three polynomials of even degree can never have the SAA Property and are therefore imprimitive.

Lemma III.6: *For any nonnegative integers* n *and* t *where* $n = 2\tilde{n}$ *and* $3 \nmid n$*, then it is the case that* $3 \nmid 2\tilde{n} + t(2^{2\tilde{n}} - 1)$.

Proof. Lemma III.5 shows $3 \mid (2^{2\tilde{n}} - 1)$ so $3 \mid t(2^{2\tilde{n}} - 1)$ for any choice of $t \in \mathbb{Z}$. Thus when $n = 2\tilde{n}$ and $3 \nmid n$, three cannot divide $2\tilde{n} + t(2^{2\tilde{n}} - 1)$ which completes the proof. □

So the degree of a row three polynomial cannot be even or a multiple of three and be primitive. By applying a sieve to the integers and removing those not of the form $n = 2\tilde{n}$ or $n = 3\tilde{n}$, we observe that the remaining integers have the form $n = 6\tilde{n} \pm 1$ for all $\tilde{n} \in \mathbb{Z}$.

~~1~~	~~2~~	~~3~~	~~4~~	**5**	~~6~~	**7**	~~8~~	~~9~~	~~10~~
11	~~12~~	**13**	~~14~~	~~15~~	~~16~~	**17**	~~18~~	**19**	~~20~~
~~21~~	~~22~~	**23**	~~24~~	**25**	~~26~~	~~27~~	~~28~~	**29**	~~30~~

Table III.1 Integers of the form $6\mathbb{Z} \pm 1$

We now prove that if $f(x)$ is a row-three polynomial with degree $n = 6\tilde{n} \pm 1$, then $f(x)$ has a SAA solution and can be further tested for the SAA Property (i.e. primitivity) using the method described in Chapter II.

Theorem III.7: *When* $n = 6\tilde{n} \pm 1$*, three divides* $6\tilde{n} \pm 1 + t(2^{6\tilde{n}\pm1} - 1)$ *for some* $t \in \{1, 2\}$.

Proof 1 (Induction). Clearly $3 \mid 6\tilde{n}$, so when $n = 6\tilde{n} - 1$ and $t = 1$ we have

$$\begin{aligned}(2^{6\tilde{n}-1} - 1) - 1 &= (2^{6\tilde{n}-1} - 2)\\ &= 2(2^{6\tilde{n}-2} - 1)\\ &= 2(2^{2(3\tilde{n}-1)} - 1).\end{aligned}$$

By Lemma III.5 three divides $(2^{2(3\tilde{n}-1)} - 1)$, so three also divides $(6\tilde{n} + 2^{6\tilde{n}-1} - 2)$.

Proof 2 (Induction). Again $3 \mid 6\tilde{n}$, so when $n = 6\tilde{n} + 1$ and $t = 2$ we have

$$\begin{aligned}2(2^{6\tilde{n}+1} - 1) + 1 &= (2^{6\tilde{n}+2} - 1)\\ &= (2^{2(3\tilde{n}+1)} - 1).\end{aligned}$$

By Lemma III.5 three divides $(2^{2(3\tilde{n}+1)} - 1)$, so three also divides $(6\tilde{n} + 2^{6\tilde{n}+2} - 1)$. Thus for any choice of $t \in \{1, 2\}$, three always divides $6\tilde{n} \pm 1 + t(2^{6\tilde{n}\pm1} - 1)$, which completes the proof. □

Combining the first and second class of row three polynomials, we obtain a generalized class of row three polynomials of the form $f(x) = x^{6\tilde{n}\pm1} + (x + 1)^k$ which, if irreducible, potentially have an associated primitive element. Before we begin searching for primitive polynomials of this type, recall from the beginning of the chapter that the generalized Pascal polynomial has the form $f(x) = x^n + (x^a + 1)^k$. Note that our solutions for the SAA pair of row three polynomials is independent of the value of a. We use this concept to find multiple pentanomials for a specific value of n which we can also test for primitivity. Thus, we consider the most generalized row three polynomials of the form $f(x) = x^{6\tilde{n}\pm1} + (x^a + 1)^k$ where $n = 6\tilde{n} \pm 1 > 3a$.

As an example, consider a row three polynomial of degree seven, where the exponent a is equal to one. This polynomial expands to the pentanomial $f(x) = x^7 + x^3 + x^2 + x + 1$. We could also allow the exponent a to equal two and the resulting polynomial is $f(x) = x^7 + x^6 + x^4 + x^2 + 1$, which is still a pentanomial of degree 7. So for polynomials of degree seven, there are two pentanomials to test for primitivity. Both of these are in fact primitive. Generalizing this concept, as long as $n > 3a$, there are $\lfloor \frac{(n-2)}{3} \rfloor$ pentanomials which may be primitive.

B. ROW FIVE POLYNOMIALS

The next class of polynomials we investigate are row five polynomials of the form $f(x) = x^n + (x+1)^5$. Note that five is one greater than a power of two, so the full expansion yields a pentanomial of the form $f(x) = x^n + x^5 + x^4 + x + 1$. Again we examine characteristics of the degree of the polynomial. If the degree is a multiple of five, then $f(x)$ is reducible.

Theorem III.8: *Given a polynomial $f(x) = x^{5\tilde{n}} + (x+1)^5$ over $GF(2)$ and $\tilde{n} > 1$, $f(x)$ is reducible with the factor $g(x) = x^n + x + 1$.*

Proof (Construction).

$$\begin{aligned} x^{5\tilde{n}} + (x+1)^5 &\equiv x^{\tilde{n}}(x^{4\tilde{n}} + (x+1)^4) + x^{\tilde{n}}(x+1)^4 + (x+1)^5 \\ &\equiv x^{\tilde{n}}(x^{\tilde{n}} + (x+1))^4 + (x+1)^4(x^{\tilde{n}} + (x+1)) \\ &\equiv (x^{\tilde{n}} + x + 1)(x^{\tilde{n}}(x^{\tilde{n}} + x + 1)^3 + (x+1)^4) \pmod{2}, \end{aligned}$$

which completes the proof. □

Next, we consider the case where the degree of $f(x)$ is a multiple of four. It follows from Fermat's Little Theorem that when the degree of the monomial term is divisible by four but not by five, then the cyclic element with exponent $2^{4\tilde{n}} - 1$ is divisible by five.

Lemma III.9: *Given an integer $n = 4\tilde{n}$ relatively prime to five, $2^{4\tilde{n}} - 1$ is divisible by five.*

Proof. By Fermat's Little Theorem,

$$\begin{aligned} (2^{5-1}) = (2^4) &\equiv 1 \pmod{5} \\ (2^4)^{\tilde{n}} &\equiv 1 \pmod{5} \\ (2^{4\tilde{n}}) - 1 &\equiv 0 \pmod{5}, \end{aligned}$$

which completes the proof. □

So a row five polynomial is never primitive if its degree is a multiple of four or five. Unfortunately we are not able to say more about when these polynomials are in fact primitive. Some of these issues are addressed in Chapter IV.

C. GENERALIZED RESULTS

Following the method described in the preceding sections, there are two main results that can be generalized as follows. The degree of a polynomial cannot be a multiple of the row value k and the degree cannot be a multiple of $\phi(k)$, where ϕ is Euler's Totient function as defined in Chapter 2. In the first case the polynomial is reducible while the second case shows imprimitivity since $f(x)$ has no SAA solution. We present these results in a consolidated theorem now.

Theorem III.10: *Given a polynomial of the form $f(x) = x^N + (x^A + 1)^K$ over $GF(2)$, where $N > KA$ and K is odd, if*

(i) $N = KT$ *for any integer* $T > A$, *then* $f(x)$ *is reducible with factor* $g(x) = x^T + x + 1$.

(ii) $N = \phi(K)T$ *for any integer* T *not a multiple of* K, *then* $f(x)$ *is imprimitive.*

Proof (i). Represent K in its binary expansion $K = 2^m + a_{m-1}2^{m-1} + \cdots + a_1 2 + 1$. By a telescoping algorithm, begin with $K = 2^m + R$ so that

$$\begin{aligned} x^{KT} + (x^A + 1)^K &= x^{(2^m+R)T} + (x^A + 1)^{(2^m+R)} \\ &= x^{RT}(x^{2^mT} + (x^A + 1)^{2^m}) + x^{RT}(x^A + 1)^{2^m} \\ &\quad + (x^A + 1)^{2^m}(x^A + 1)^R \\ &= x^{RT}(x^T + x^A + 1)^{2^m} + (x^A + 1)^{2^m}(x^{RT} + (x^A + 1)^R). \end{aligned}$$

Repeat this process on the $(x^{RT} + (x^A + 1)^R)$ term for each nonzero a_i coefficient until $K_j = 2^j + 1$.

Proof (ii). Assume $f(x)$ is a primitive polynomial of degree $N = \phi(K)T$, where T is not a multiple of K, over $GF(2)$ with root α. Then $f(\alpha) = \alpha^N + (\alpha^A + 1)^K = 0$, and $(\alpha^A + 1)^K = \alpha^N \alpha^{L(2^N-1)}$. Since K does not divide N, it is sufficient to show that if K divides $L(2^N - 1)$, then $f(x)$ has no SAA solution and is never primitive. The result follows directly from Euler's Theorem. Since K is odd, K is relatively prime to 2. Thus,

$$\begin{aligned} 2^{\phi(K)} &\equiv 1 \pmod{K} \\ 2^N = 2^{\phi(K)T} = (2^{\phi(K)})^T &\equiv 1 \pmod{K} \\ 2^{\phi(K)T} - 1 &\equiv 0 \pmod{K} \end{aligned}$$

and K divides $(2^N - 1)$, which completes the proof. □

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RESULTS AND FUTURE WORK

We have shown that primitive polynomials of the form $f(x) = x^n + p(x)$, where $p(x)$ is a certain row of Pascal's triangle modulo 2, have restrictions on the value of n for a given k^{th} row. Although this thesis presents conditions under which a polynomial cannot be primitive, we have not stated anything conclusive about when a polynomial definitely is primitive. The data presented in Appendices C - F, demonstrates that the actual number of primitive polynomials to the outside solutions ($n > a \cdot k$) is not nearly as dense as we had hoped. In fact , for a fixed row k of Pascal's triangle, the number of primitive polynomials as n increases becomes very sparse. Perhaps as n grows, so too must the row of the triangle which we evaluate.

Although we did not discuss "inside" solutions in Chapter 3, such a polynomial occurs when the degree of the monomial term is inside the expanded binomial terms such that $n < a \cdot k$ and the degree is therefore $a \cdot k$ (by our notation for the general form of a Pascal polynomial). For example, the polynomial

$$\begin{aligned} f_p(x) &= (x+1)^9 + x^4 \\ &= x^9 + x^8 + x^4 + x + 1 \end{aligned}$$

is an inside polynomial and is in fact primitive. We performed a comparison of these polynomials to trinomials of equal degrees, with interesting results (Appendices G - H). The results indicate that any primitive Pascal polynomial has an identical, corresponding primitive trinomial. For example, if the polynomial $f(x) = (x+1)^k + x^n$ is primitive, then the trinomial $t(x) = x^k + x^n + 1$ is also primitive. So given our example of f_p above, the trinomial $f_t(x) = x^9 + x^4 + 1$ should also be primitive, which it is.

Our experimental result is indicative of the theoretical results obtained by Zeng , Han, and He in their currently unpublished paper, *The parity of the number of irreducible factors of* $x^{l-ef}(x^f + 1)^e + 1$ *over* $\mathbb{F}_2$ [11]. In this paper, the authors present a generalization of Swan's theorem for our Pascal polynomials similar to those made in the paper by Fredricksen, Hales, and Sweet [6] for trinomials. It is not immediately apparent that the polynomials of the form $x^{l-ef}(x^f+1)^e+1$ are equivalent to our polynomials with the form $x^n + (x^a + 1)^k$, but they are in fact reciprocal polynomials.

One area of future work lies in further analysis of the results regarding those Pascal polynomials that are primitive. Is there a trend that we can depict, by graphical or other means, which might lend some insight into a method of predicting when a Pascal polynomial will be primitive? Given the linear nature of polynomials as LFSRs, stream ciphers using this technique are relatively easy to break for small degree polynomials. However, as the degree becomes very large, say $n \geq 200$, the sequences take an incredibly long time to repeat. In fact, a 200 degree polynomial with full period would take approximately 6.22×10^{48} years to recycle with a data rate of 1 megabit/second. If we could efficiently find a large pool of polynomials with large degree, we could utilize portions of LFSRs with a reasonable level of security.

APPENDIX A. PROOF OF PRIMITIVE POLYNOMIAL ALGORITHM

Given a polynomial $f(x)$ of degree n over $GF(2)$, such that $n > 2$, we know the period of $f(x)$, denoted per($f(x)$), is less than or equal to $2^n - 1$. We also know $f(x)$ is primitive if the period of $f(x) = 2^n - 1$. And we know that given two polynomials $p(x)$ and $q(x)$, the per$(p(x)q(x)) =$ lcm(per$(p(x))$, per$(q(x)))$. Armed with these facts, we are prepared to make and prove the following claim.

Theorem A.1: *Given a polynomial $f(x)$ of degree n over $GF(2)$, and $x^{2^n-1} \equiv 1 \pmod{f(x)}$, and $x^d \not\equiv 1 \pmod{f(x)}$, for all d that are divisors of $2^n - 1$, then $f(x)$ is primitive.*

Proof (Contradiction). If we know $f(x)$ to be irreducible of degree n, we know per$(f(x))|2^n - 1$. So if we know that $f(x)$ is irreducible, then the conditions $x^{2^n-1} \equiv 1 \pmod{f(x)}$ and $x^d \not\equiv 1 \pmod{f(x)}$ imply that $f(x)$ is primitive. But we don't know that $f(x)$ is irreducible.

It is sufficient to show that there exists some $d|2^n - 1$ such that $x^d \equiv 1 \pmod{f(x)}$. Let's assume that $f(x) = g(x)h(x)$, where $0 <$ deg$(g(x)) = r < n$, and $0 <$ deg$(h(x)) = s < n$, and deg$(f(x)) =$ deg$(g(x)) +$ deg$(h(x)) = r + s = n$, and $\gcd(g(x), h(x)) = 1$, and $x^{2^n-1} \equiv 1 \pmod{f(x)}$. Then per$(g(x)) = e_1 \leq 2^r - 1$ and per$(h(x)) = e_2 \leq 2^s - 1$. So per $(f(x)) =$ lcm$(e_1, e_2) = e$, and

$$e \leq (2^r - 1)(2^s - 1) = 2^{r+s} - 2^r - 2^s + 1 < 2^n - 1$$

But, since $g(x)|f(x)$ and $f(x)|x^{2^n-1} + 1$, it is also the case that $g(x)|x^{2^n-1} + 1$, which implies that $e_1|2^n - 1$. By a similar arguement, $h(x)|f(x)$ so $h(x)|x^{2^n-1} + 1$, which implies that $e_2|2^n - 1$. Now, since $e_1|2^n - 1$ and $e_2|2^n - 1$, we know that $e|2^n - 1$. But $e < 2^n - 1$, so $h(x)|x^e + 1$ and $g(x)|x^e + 1$ which implies that $f(x)|x^e + 1$. Therefore $e = 2^d - 1 < 2^n - 1$ and $f(x)$ is imprimitive. Thus the contradiction which completes the proof. □

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. SAMPLE MAGMA CODE

This appendix is an example of the code used in Magma, an algebraic software package, to test values of N from 1 to 750 for a given line of Pascal's triangle. The sample code below is from a third row polynomial and the code includes the two checks discovered in the thesis to filter values of N. This code checks for primitivity, but could also be used to check for irreducibility.

```
P<x> := PolynomialRing(GF(2));

for n in [1..700] do
  t := n mod 6;
  if t eq 1 or t eq 5 then
    max := Floor(n/3);
    n, { a: a in [1..max] | IsPrimitive(f) where f\\
    is x^n + (x^a +1)^3 };
  end if;
end for;
```

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX C. PRIMITIVE TRINOMIALS

This appendix presents all primitive trinomials of degree four to 750. The trinomials have the form $x^N + x^K + 1$. If there are multiple values in the K cell, then each choice of K for the corresponding N is a primitive trinomial. We do not list the reciprocal polynomials, so we only test values of K up to $\lfloor \frac{N}{2} \rfloor$.

Table C.1: Primitive trinomials of degree 4 to 750.

N	K	N	K	N	K
4	1	249	86	489	83
5	2	250	103	490	219
6	1	252	67	494	137
7	1, 3	255	52, 56, 82	495	76, 89, 118, 226
9	4	257	12, 41, 48, 51, 65	497	78, 216, 228
10	3	258	83	503	3, 26, 248
11	2	263	93	505	156, 174
15	1, 4, 7	265	42, 127	506	95, 135
17	3, 5, 6	266	47	508	109
18	7	268	25, 61	511	10, 15, 31, 160, 202, 216
20	3	270	53, 133	513	85, 175
21	2	271	58, 70	518	33, 45
22	1	273	23, 53, 67, 88, 92, 110, 113	519	79
23	5, 9	274	67, 99, 135	521	32, 48, 158, 168
25	3, 7	278	5	524	167
28	3, 9, 13	279	5, 10, 38, 40, 41, 59, 76, 80, 125	527	47, 123, 147, 152, 198, 239
29	2	281	93, 99	529	42, 114, 157
31	3, 6, 7, 13	282	35, 43	532	1, 37
33	13	284	119	537	94
35	2	286	69, 73	540	179, 211
36	11	287	71, 116, 125	543	16, 28, 58, 203, 235
39	4, 8, 14	289	21, 36, 84	545	122
41	3, 20	292	97	550	193
47	5, 14, 20, 21	294	61	551	135, 240
49	9, 12, 15, 22	295	48, 112, 123, 142, 147	553	39, 57, 94, 99, 109, 255, 258
52	3, 19, 21	297	5, 83, 103, 122, 137	556	153
55	24	300	7, 73, 91	559	34, 70, 148, 210
57	7, 22	302	41	561	71, 109, 155
58	19	305	102	564	163
60	1, 11	313	79, 121	566	153
63	1, 5, 31	314	15	567	143, 275
65	18, 32	316	135	569	77, 210
68	9, 33	319	36, 52, 129	570	67
71	6, 9, 18, 20, 35	321	31, 56, 76, 82, 155	574	13
73	25, 28, 31	322	67	575	146
79	9, 19	327	34, 152	577	25, 27, 231
81	4, 16, 35	329	50, 54	582	85

Continued on Next Page…

Table C.1 – Continued

N	K	N	K	N	K
84	13	332	123	583	130
87	13	333	2	585	121, 151, 157, 232
89	38	337	55, 57, 135, 139, 147	588	151, 253
93	2	342	125	590	93
94	21	343	75, 135, 138, 159	593	86, 108, 119, 177
95	11, 17	345	22, 37, 106	594	19, 35
97	6, 12, 33, 34	350	53	599	30, 210
98	11, 27	351	34, 55, 116, 134	601	201, 202
100	37	353	69, 95, 138, 143, 153, 173	607	105, 147, 273
103	9, 13, 30, 31	359	68, 117	609	31, 128, 181, 233
105	16, 17, 37, 43, 52	362	63, 107	610	127
106	15	364	67	615	211, 232, 238
108	31	366	29	617	200
111	10, 49	367	21, 171	622	297
113	9, 15, 30	369	91, 110	623	68, 87, 128, 185, 230, 251, 296, 311
118	33, 45	370	139, 183	625	133, 156
119	8, 38	375	16, 64, 149, 182	628	223, 289
121	18	377	41, 75	631	307
123	2	378	43, 107	633	101, 292
124	37	380	47	634	315
127	1, 7, 15, 30, 63	382	81	639	16, 88, 95, 179, 305
129	5, 31, 46	383	90, 108, 135	641	11, 36, 45, 95, 287
130	3	385	6, 24, 51, 54, 142, 159	642	119
132	29	386	83	646	249
134	57	390	89	647	5, 150, 215, 312
135	11, 16, 22	391	28, 31	649	37, 73, 171, 310, 321
137	21, 35, 57	393	7, 62, 91	650	3
140	29	394	135	652	93, 97
142	21	396	25, 109, 169, 175	655	88, 192
145	52, 69	399	86, 109, 181	657	38, 92, 148
148	27	401	152, 170	658	55
150	53	404	189	662	297
151	3, 9, 15, 31, 39, 43, 46, 51, 63, 66, 67, 70	406	157	663	257, 307
153	1, 8	407	71, 105	665	33, 53, 144, 192, 269, 317
159	31, 34, 40	409	87	670	153, 273
161	18, 39, 60	412	147	671	15, 201, 243
167	6, 35, 59, 77	415	102, 163	673	28, 183, 252, 259, 300
169	34, 42, 57, 84	417	107, 113, 155	676	241, 277
170	23	422	149	679	66, 216
172	7	423	25	686	197
174	13	425	12, 21, 42, 66, 111, 191	687	13, 133
175	6, 16, 18, 57	428	105	689	14, 87, 179, 207, 336
177	8, 22, 88	431	120, 200	692	299
178	87	433	33, 61, 118, 153	695	212
183	56	436	165	697	267, 310
185	24, 41, 69	438	65	698	215, 311
191	9, 18, 51, 71	439	49, 133, 145, 156, 171	702	37, 317
193	15, 73, 85	441	31, 127, 212	705	19, 161, 194, 266, 328, 331
194	87	446	105, 153	708	287, 301
198	65	447	73, 83	711	92
199	34, 67	449	134, 167	713	41, 297

Continued on Next Page…

Table C.1 – Continued

N	K	N	K	N	K
201	14, 17, 59, 79	450	79	714	23, 151
202	55	455	38, 62, 74	716	183, 275
207	43	457	16, 61, 123, 210, 217, 226	719	150, 174, 257, 299, 314
209	6, 8, 14, 45, 47, 50, 62	458	203	721	9, 159, 256, 270, 283, 328
212	105	460	61	722	231
215	23, 51, 63, 77, 101	462	73	726	5, 241
217	45, 64, 66, 82, 85	463	93, 168, 214	727	180, 217, 357
218	11, 15, 71, 83	465	59, 103, 158	729	58, 253
223	33, 34, 64, 70, 91	470	149, 177	730	147
225	32, 74, 88, 97, 109	471	1, 119, 127	735	44, 89, 262
231	26, 34	474	191, 215	737	5, 303
233	74	476	15, 141	738	347
234	31, 103	478	121	740	153, 317
236	5	479	104, 105, 122, 158, 224	743	90, 144, 146, 209, 210, 239, 279, 326
239	36, 81	481	138, 201, 231	745	258, 336, 342
241	70	484	105	746	351
247	82, 102	487	94, 127		

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX D. PRIMITIVE INSIDE PASCAL POLYNOMIALS

This appendix presents all primitive inside Pascal polynomials of degree four to 750. The trinomials have the form $(x{+}1)^N{+}x^K$, where $N > K$. If there are multiple values in the K cell, then each choice of K for the corresponding N is a primitive polynomial. We do not list the reciprocal polynomials, so we only test values of K up to $\lfloor \frac{N}{2} \rfloor$.

Table D.1: Primitive inside Pascal polynomials of degree 4 to 750.

N	K	N	K	N	K
4	1	249	86	489	83
5	2	250	103	490	219
6		252		494	137
7	1, 3	255	52, 56, 82	495	76, 89, 118, 226
9	4	257	12, 41, 48, 51, 65	497	78, 216, 228
10	3	258		503	3, 26, 248
11	2	263	93	505	156, 174
15	1, 4, 7	265	42, 127	506	
17	3, 5, 6	266	47	508	109
18		268	25, 61	511	10, 15, 31, 160, 202, 216
20		270		513	85, 175
21		271	58, 70	518	33, 45
22	1	273		519	79
23	5, 9	274	67, 99, 135	521	32, 48, 158, 168
25	3, 7	278	5	524	167
28	3, 9, 13	279	5, 10, 38, 40, 41, 59, 76, 80, 125	527	47, 123, 147, 152, 198, 239
29	2	281	93, 99	529	42, 114, 157
31	3, 6, 7, 13	282		532	1, 37
33	13	284	119	537	94
35	2	286	69, 73	540	
36		287	71, 116, 125	543	16, 28, 58, 203, 235
39	4, 8, 14	289	21, 36, 84	545	122
41	3, 20	292	97	550	
47	5, 14, 20, 21	294		551	135, 240
49	9, 12, 15, 22	295	48, 112, 123, 142, 147	553	39, 57, 94, 99, 109, 255, 258
52	3, 19, 21	297	5, 83, 103, 122, 137	556	153
55	24	300		559	34, 70, 148, 210
57	7, 22	302	41	561	71, 109, 155
58	19	305	102	564	
60		313	79, 121	566	153
63		314	15	567	
65	18, 32	316	135	569	77, 210
68	9, 33	319	36, 52, 129	570	
71	6, 9, 18, 20, 35	321	31, 56, 76, 82, 155	574	13
73	25, 28, 31	322	67	575	146
79	9, 19	327	34, 152	577	25, 27, 231

Continued on Next Page…

Table D.1 – Continued

N	K	N	K	N	K
81	4, 16, 35	329	50, 54	582	
84		332	123	583	130
87	13	333	2	585	121, 151, 157, 232
89	38	337	55, 57, 135, 139, 147	588	
93	2	342		590	93
94	21	343	75, 135, 138, 159	593	86, 108, 119, 177
95	11, 17	345	22, 37, 106	594	
97	6, 12, 33, 34	350	53	599	30, 210
98	11, 27	351	34, 55, 116, 134	601	201, 202
100		353	69, 95, 138, 143, 153, 173	607	105, 147, 273
103	9, 13, 30, 31	359	68, 117	609	
105		362	63, 107	610	127
106	15	364	67	615	211, 232, 238
108		366		617	200
111	10, 49	367	21, 171	622	297
113	9, 15, 30	369	91, 110	623	68, 87, 128, 185, 230, 251, 296, 311
118	33, 45	370	139, 183	625	133, 156
119	8, 38	375	16, 64, 149, 182	628	223, 289
121	18	377	41, 75	631	307
123	2	378		633	101, 292
124	37	380		634	315
127	1, 7, 15, 30, 63	382	81	639	16, 88, 95, 179, 305
129	5, 31, 46	383	90, 108, 135	641	11, 36, 45, 95, 287
130	3	385	6, 24, 51, 54, 142, 159	642	
132		386	83	646	249
134	57	390		647	5, 150, 215, 312
135	11, 16, 22	391	28, 31	649	37, 73, 171, 310, 321
137	21, 35, 57	393	7, 62, 91	650	3
140		394	135	652	93, 97
142	21	396		655	88, 192
145	52, 69	399		657	
148	27	401	152, 170	658	55
150		404	189	662	297
151	3, 9, 15, 31, 39, 43, 46, 51, 63, 66, 67, 70	406	157	663	257, 307
153	1, 8	407	71, 105	665	33, 53, 144, 192, 269, 317
159	31, 34, 40	409	87	670	153, 273
161	18, 39, 60	412	147	671	15, 201, 243
167	6, 35, 59, 77	415	102, 163	673	28, 183, 252, 259, 300
169	34, 42, 57, 84	417	107, 113, 155	676	241, 277
170	23	422	149	679	66, 216
172	7	423	25	686	197
174		425	12, 21, 42, 66, 111, 191	687	13, 133
175	6, 16, 18, 57	428	105	689	14, 87, 179, 207, 336
177	8, 22, 88	431	120, 200	692	299
178	87	433	33, 61, 118, 153	695	212
183	56	436	165	697	267, 310
185	24, 41, 69	438		698	215, 311
191	9, 18, 51, 71	439	49, 133, 145, 156, 171	702	
193	15, 73, 85	441		705	19, 161, 194, 266, 328, 331
194	87	446	105, 153	708	
198		447	73, 83	711	92

Continued on Next Page…

Table D.1 – Continued

N	K	N	K	N	K
199	34, 67	449	134, 167	713	41, 297
201	14, 17, 59, 79	450		714	
202	55	455	38, 62, 74	716	183, 275
207	43	457	16, 61, 123, 210, 217, 226	719	150, 174, 257, 299, 314
209	6, 8, 14, 45, 47, 50, 62	458	203	721	9, 159, 256, 270, 283, 328
212	105	460		722	231
215	23, 51, 63, 77, 101	462		726	
217	45, 64, 66, 82, 85	463	93, 168, 214	727	180, 217, 357
218	11, 15, 71, 83	465		729	58, 253
223	33, 34, 64, 70, 91	470	149, 177	730	147
225	32, 74, 88, 97, 109	471	1, 119, 127	735	
231		474		737	5, 303
233	74	476	15, 141	738	
234		478	121	740	
236	5	479	104, 105, 122, 158, 224	743	90, 144, 146, 209, 210, 239, 279, 326
239	36, 81	481	138, 201, 231	745	258, 336, 342
241	70	484	105	746	351
247	82, 102	487	94, 127		

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX E. PRIMITIVE ROW THREE PASCAL POLYNOMIALS

This appendix presents all primitive row three Pascal polynomials of degree four to 750. The polynomials have the form $x^N + (x^A + 1)^3$. If there are multiple values in the A cell, then each choice of A for the corresponding N is a primitive polynomial.

Table E.1: Primitive row three Pascal polynomials of degree 4 to 750.

N	A	N	A	N	A
5	1	217	15, 22, 44, 45, 51	463	31, 56, 83
7	1, 2	223	11, 44, 51, 53, 63	479	35, 85, 107, 119, 125
11	3	233	53	481	46, 67, 77
17	1, 2, 4	239	12, 27	487	120, 131
23	3, 6	241	57	497	26, 72, 76
25	1, 6	247	34, 55	503	1, 85, 159
29	9	257	4, 16, 17, 64, 72	505	52, 58
31	1, 2, 6, 8	263	31	511	5, 72, 103, 117, 160, 167
35	11	265	14, 46	521	16, 56, 121, 163
41	1, 7	271	67, 71	527	41, 49, 66, 96, 125, 160
47	7, 9, 11, 14	281	31, 33	529	14, 38, 124
49	3, 4, 5, 9	287	54, 57, 72	545	141
55	8	289	7, 12, 28	551	45, 80
65	6, 11	295	16, 41, 49, 51, 61	553	13, 19, 33, 85, 86, 148, 153
71	2, 3, 6, 12, 17	305	34	559	70, 137, 163, 175
73	14, 15, 16	313	64, 78	569	70, 164
79	3, 20	319	12, 43, 89	575	143
89	17	329	18, 93	577	9, 77, 184
95	26, 28	337	19, 45, 49, 66, 94	583	151
97	2, 4, 11, 21	343	25, 45, 46, 53	593	36, 59, 158, 169
103	3, 10, 24, 30	353	23, 46, 51, 60, 70, 86	599	10, 70
113	3, 5, 10	359	39, 97	601	67, 133
119	27, 37	367	7, 57	607	35, 49, 91
121	6	377	25, 112	617	139
127	5, 10, 21, 40, 42	383	30, 36, 45	623	29, 104, 109, 124, 131, 146, 165, 185
137	7, 19, 34	385	2, 8, 17, 18, 53, 81	625	52, 164
145	23, 31	391	120, 121	631	108
151	1, 3, 5, 13, 17, 21, 22, 27, 28, 35, 36, 40	401	77, 83	641	12, 15, 118, 182, 210
161	6, 1 3, 20	407	35, 112	647	50, 104, 144, 214
167	2, 30, 36, 44	409	29	649	57, 107, 113, 192, 204
169	14, 19, 28, 45	415	34, 84	655	64, 189
175	2, 6, 19, 53	425	4, 7, 14, 22, 37, 78	665	11, 48, 64, 116, 132, 204
185	8, 23, 48	431	40, 77	671	5, 67, 81
191	3, 6, 17, 40	433	11, 51, 105, 124	673	61, 84, 100, 138, 215
193	5, 36, 40	439	52, 57, 98, 102, 130	679	22, 72
199	44, 55	449	94, 105	689	29, 69, 112, 170, 225

Continued on Next Page…

Table E.1 – Continued

N	A	N	A	N	A
209	2, 15, 49, 53, 54, 65, 67	455	127, 131, 139	695	161
215	17, 21, 38, 46, 64	457	41, 70, 77, 80, 132, 147	697	89, 129

APPENDIX F. PRIMITIVE ROW FIVE PASCAL POLYNOMIALS

This appendix presents all primitive row five Pascal polynomials of degree six to 750. The polynomials have the form $x^N + (x^A + 1)^5$. If there are multiple values in the A cell, then each choice of A for the corresponding N is a primitive polynomial.

Table F.1: Primitive row five Pascal polynomials of degree 6 to 750.

N	A	N	A	N	A
6	1	258	35	471	94
9	1	263	34	474	43
17	1	271	14	479	21, 51, 75
23	1	273	22, 32, 37, 44, 50	481	50, 56
31	5	274	27, 35	487	72
33	4	278	1	503	51, 100
39	5, 7	279	1, 2, 8, 16, 25, 44	506	19, 27
41	4	282	7	511	2, 3, 32, 59, 96
47	1, 4	287	25	513	17, 35
49	3, 8	289	41	518	9, 97
57	7, 10	297	1, 32, 35	519	88
63	1	314	3	527	75, 76, 96
71	4, 7, 13	319	38	529	83
73	5, 9	321	31, 49, 53, 58	543	47, 68, 97, 103
79	12, 14	322	51	551	27, 48
81	7, 13	327	35	553	51, 59
97	17	329	10, 55	559	14, 42, 105
103	6, 18	337	11, 27, 38, 56	561	31, 98
106	3	342	25	567	55
111	2	343	15, 27, 41	569	42
113	3, 6	351	11, 47	577	5, 110
118	9, 17	353	19, 36, 40, 42, 43	582	17
127	3, 6, 24	362	51	583	26
129	1	369	22	593	97
137	7, 16	377	15	594	7, 115
151	3, 14, 17, 20, 21, 24	378	67	599	6, 42
153	29	383	18, 27, 55	601	80
159	8, 25	391	72	607	21, 92
161	12	394	27	617	40
167	7, 18	399	58	622	65
169	17, 27	401	34	623	37, 46, 99, 111
177	31	407	21	634	63
191	24, 28	417	31, 62	639	19, 61, 92
193	3, 17, 24	423	5	641	9, 19, 121, 126
198	13	431	24, 40	647	1, 30, 43, 67
199	33	433	56, 63, 80	649	62
202	11	438	13	657	113
209	9, 10, 39	439	29, 78	658	11

Continued on Next Page…

Table F.1 – Continued

N	A	N	A	N	A
217	9, 17, 27	441	82	662	73
218	3, 27	446	21	671	3, 94
223	14, 38	449	63	673	60, 98, 129
231	41	457	42, 48	689	102, 135
241	14	458	51	697	62, 86
247	29, 33	463	59, 74	698	43
257	13, 49				

APPENDIX G. PRIMITIVE ROW SEVEN PASCAL POLYNOMIALS

This appendix presents all primitive row seven Pascal polynomials of degree eight to 750. The polynomials have the form $x^N + (x^A + 1)^7$. If there are multiple values in the A cell, then each choice of A for the corresponding N is a primitive polynomial.

Table G.1: Primitive row seven Pascal polynomials of degree 8 to 750.

N	A	N	A	N	A
10	1	239	29	457	30, 31, 33, 63
17	2	241	10	458	29
22	3	250	21	460	57
23	2	257	35	463	24
25	1	265	6	478	51
31	1, 4	271	10	479	15, 32, 51
41	3	274	25	481	33, 40, 49
47	2, 3, 6	278	39	484	15
52	3, 7	281	26	494	51
68	5	284	17	506	53
71	5	286	31	508	57
73	4, 6	289	3, 12	521	24
79	10	295	16, 21	524	51
94	3	305	29	527	21, 47
95	12	337	21, 40	529	6
97	9, 13	353	30	550	51
100	9	362	9	559	10, 30, 75
106	13	367	3, 28	566	59
113	14	370	33	569	11, 30
127	1, 9, 16, 18	377	48	577	33
134	11	382	43	590	71
137	3, 5	391	4	593	17
142	3	394	37	599	30
151	9, 10, 12, 15, 16	401	33	601	57
167	5, 11, 23	404	27	607	15, 21, 39
169	6, 12, 16	407	15, 48	610	69
170	21	409	46	625	19, 67
172	1	412	21	634	45
178	13	415	36	641	41, 78, 90
185	23	422	39	647	71
191	20, 26	425	3, 6, 59	655	81
202	21	428	15	670	39
209	2, 21, 29	431	33	673	4, 36, 37, 70
212	15	433	40, 45	676	57
215	9, 11	439	7, 19, 42	689	2, 48, 86
218	21, 29	446	15	695	69

Continued on Next Page…

Table G.1 – Continued

N	A	N	A	N	A
223	10, 13, 27	449	45	698	69
236	33				

APPENDIX H. PRIMITIVE ROW NINE PASCAL POLYNOMIALS

This appendix presents all primitive row nine Pascal polynomials of degree ten to 750. The polynomials have the form $x^N + (x^A + 1)^9$. If there are multiple values in the A cell, then each choice of A for the corresponding N is a primitive polynomial.

Table H.1: Primitive row nine Pascal polynomials of degree 10 to 750.

N	A	N	A	N	A
11	1	209	5, 18	439	19, 34
23	1, 2	215	7	449	35
25	2	217	5, 15, 17	457	44, 49
29	3	223	17, 21	487	40
31	2	239	4, 9	497	24
47	3	241	19	503	53
49	1, 3	257	24	511	24, 39
65	2	281	11	527	22, 32
71	1, 2, 4	287	18, 19, 24	545	47
73	5	289	4	551	15
79	1	295	17	553	11, 51
97	7	313	26	577	3
103	1, 8, 10	319	4	593	12
113	1	329	6, 31	623	55
119	9	337	15, 22	631	36
121	2	343	15	641	4, 5, 70
127	7, 14	353	17, 20	647	48
151	1, 7, 9, 12	359	13	649	19, 64, 68
161	2	367	19	655	63
167	10, 12	383	10, 12, 15	665	16, 44, 68
169	15	385	6, 27	671	27
175	2	391	40	673	28, 46
185	16	415	28	679	24
191	1, 2	425	26	689	23, 75
193	12	433	17, 35	697	43

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX I. PRIMITIVE ROW ELEVEN PASCAL POLYNOMIALS

This appendix presents all primitive row eleven Pascal polynomials of degree twelve to 750. The polynomials have the form $x^N + (x^A + 1)^{11}$. If there are multiple values in the A cell, then each choice of A for the corresponding N is a primitive polynomial.

Table I.1: Primitive row eleven Pascal polynomials of degree 12 to 750.

N	A	N	A	N	A
15	1	215	7	447	34
17	1	217	6, 12	457	21, 36
18	1	218	1	471	32
25	2	223	3, 12	478	11
35	3	225	8	479	34
36	1	236	21	481	21
47	3	247	15	518	3, 43
49	2	257	19	519	40
52	3	273	8, 10, 20	521	33, 43
57	2	274	9	527	18
65	3	279	14, 20	532	45
68	3	281	9	543	28
81	7	284	15	553	9
95	1	289	23	567	13, 25
97	3	313	11	569	7
98	1	329	25	574	51
105	8	332	19	575	39
108	7	337	5, 18	577	21, 50
118	3	345	2, 28	585	11
123	11	351	5	588	23
134	7	353	13	622	27
135	1, 2	359	22	623	45
142	11	364	27	633	31
148	11	369	10	634	29
151	6, 8	383	25	639	8
161	13	391	33	641	1, 55
167	7, 12	401	21	655	8
172	15	425	6	658	5
177	2, 8	431	21	662	27
199	12, 15	433	3	665	3, 36, 43
201	17	436	15	679	6
202	5	446	31		

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

[1] S. Golomb. *Shift Register Sequences*. Holden-Day, Inc., San Francisco, CA, 1967.

[2] National Institute of Standards & Technology. Fips-197: Specification for the advanced encryption standard (aes). *http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf*, Nov 2001.

[3] A. J. Menezes, I. F. Blake, and et al. *Applications of Finite Fields*. Kluwer Academic Publishers, Boston, MA, 1993.

[4] H. M. Fredricksen. *Cryptography Class Notes*. Naval Postgraduate School, Monterey, CA, 2006.

[5] Richard G. Swan. Factorization of polynomials over finite fields. *Pacific Journal of Mathematics*, 12(3):1099–1106, 1962.

[6] H. M. Fredricksen, A. W. Hales, and M. M. Sweet. A generalization of Swan's theorem. *Mathematics of Computation*, 46(173):321–331, Jan 1986.

[7] H. M. Fredricksen and R. Wisniewski. On trinomials $x^n + x^2 + 1$ and $x^{8l\pm3} + x^k + 1$ irreducible over $GF(2)$. *Information and Control*, 50(1):58–63, Jul 1981.

[8] J. Beachy and D. Blair. *Abstract Algebra*. Waveland Press, Inc., Long Grove, IL, 3rd edition, 2006.

[9] K. Rosen. *Elementary Number Theory*. Addison-Wesely, San Francisco, CA, 5th edition, 2005.

[10] S. E. O'Connor. Computing primitive polynomials - theory and algorithm. http://www.seanerikoconnor.freeservers.com/Mathematics/AbstractAlgebra/Primitive Polynomials/theory.html.

[11] Guang Zeng, Wenbao Han, and Kaicheng He. The parity of the number of irreducible factors of $x^{l-ef}(x^f + 1)^e + 1$ over $\mathbb{F}_2$. Unpublished.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, VA

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, CA

3. Department Chairman, Code MA
   Naval Postgraduate School
   Monterey, CA

4. Professor H. Fredricksen, Code MA
   Naval Postgraduate School
   Monterey, CA

5. Professor P. Stanica, Code MA
   Naval Postgraduate School
   Monterey, CA

6. Major C. Fernandez
   United States Military Academy, D/MATH
   West Point, NY